E-Authentication PKI Application

Applicant Point of Contact:
Applicant Phone Number:
Reason for Requesting Certificate:
Applicant Point of Contact:
Proposed Credential: (i.e., CSP level 1, CSP level 2, and AA)
Description of Operational Environment:

The rest of this application serves a checklist for the E-Authentication Initiative to provide appropriate validation services.

Background

An applicant that plans to use the E-Authentication Multi-Protocol Validation Service (MPVS) must satisfy each of the following steps before officially using the MPVS.

Policy Acceptance

The applicant must understand their legal obligations (if any) for archiving validation responses, and for advanced filing of System of Records notifications.

Certificate Acceptance

The applicant must understand the certificate profiles and other issues related to the issuing CA's operation and validation procedures, as discussed in the Applicant Technical Issues Check List Addendum below.

Technical Interoperability Testing

An applicant must first test with the development MPVS to ensure:

- The applicant's software can process the end-entity certificates
- The applicant's software can process MPVS responses
- The stunnel certificates (issued by the MPVS) are issued and installed properly (and know when the certificate will expire)
- The AA-ID field is set properly in the MPVS requests

Applicant Technical Issues Addendum

This addendum deals only with the *technical* issues that must be considered by an applicant before accepting a Certificate Authority's (CA) certificate. The answer to the following questions will determine how the validation service needs be configured.

Applicant's Certificate Authority

1. Are you willing to accept *all* end-entity certificates issued by that CA?
   a. If not, how can one distinguish between acceptable and unacceptable certs issued by the same CA? (e.g., by certificate policy Object Identifiers [OIDs]?)

2. Does the CA make validity statements about its issued certificates via Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL)?
   a. Is the OCSP responder or CRL directory open to everyone or is access restricted? If restricted, what are the criteria for access?

3. How many bits are in the CA's public key? Can your system validate a signature of that size?
   a. Windows NT systems purchased outside North American can process a maximum of a 1028-bit key in hardware. Longer keys require additional cryptographic processing hardware
   b. Windows 2000 systems can process a maximum of a 2048-bit key in software

End-Entity Certificates

1. How will you uniquely identify the holder of that end-entity certificate?
   a. An email address may or may not be present in every certificate. (Check the issuing CA's profile to be sure.) An email address may appear in the subject Domain Name (DN) string or in the "Subject Alt Name" extension. Your software should be able to read the email address from both locations.

    b. To uniquely identify an end-entity certificate is to take the SHA1 hash of the concatenation of the following certificate fields: issuer DN; the subject's public key; and the issuer's signature.

2. Is the issuing's CA validation method stated in the end-entity certificate. That is, does the certificate contain CRL Distribution Point [CDP] field designating an LDAP-compliant directory location, or an Authority Information Access [AIA] field designating the OCSP responder location?

Validation Requirements

1. Is it sufficient to validate only the end-entity certificate, or do you also need to validate the issuing CA?

2. Do you need to validate an entire trust path back to a TrustAnchor, thus requiring path discovery? Which TrustAnchor?

3. Do you need to have the location of the issuing CA's validation responder embedded in the certificate in question? Must that location be a URL, or will only the DN portion of a LDAP/X.500 directory suffice?

4. Is the OCSP response or CRL(s) signed by the issuing CA or another authority deligated by the CA? (If the latter, please contact your application manager for an address to send that certificate out-of-band to the validation service.)

5. If CRLs are employed, is processing one CRL sufficient to determine a certificate’s status, or must multiple CRLs be processed? (i.e., does the Issuing Distribution Point [IDP] extension appear in the CRL?)

6. If trust path discovery/validation is required, is any trust path acceptable, or should the path be constrained w.r.t. path length or CA names along the path (e.g., excluding trust paths through non-U.S. government CAs)?

Applicant Technical Issues Addendum

Additional Acceptability Criteria

1. Is it necessary to constrain the acceptance of an end-entity certificate based on certificate policy OID? Where do you anticipate that filtering occuring: at the applicant application or at the validation service (e.g., during trust path discovery/validation)?

Applicant's Validation Service

1. Can the validation service (VS) parse the certificates to find the CRL and/or AIA fields?

2. Can the VS properly process the CRL and/or AIA fields?

3. If there are multiple entries within one CRL or AIA field, if the processing of the first entry fails, will the VS gracefully try the other entries before responding?

4. Does the VS cache CRLs until they expire, or for some VS-specified time, or is a fresh CRL retrieved each time?

5. If trust path validation is required, does the VS allow the applicant to specify the trust anchor, or does the VS management organization assign the trust anchor?

6. Are the LDAP/X.500 directories and/or the OCSP responders open to all incoming queries, or does some access control method (e.g., firewall, or mutually-authenticated VPN) restrict access? If the latter, are the directory and responder owners willing to grant your organization access, and will that access accommodate your mobile users?